主旨: FW:[新病毒通知]最新勒索病毒RANSOM_WANA.A攻擊以及趨勢科技防護策略
從: "alan" <alan@mail.cyhg.gov.tw>
日期: 2017/5/14 下午 07:50
到: "陳伯升" <linuns@mail.cyhg.gov.tw>

—[新病毒通知]最新勒索病毒RANSOM_WANA.A.eml

主旨: [新病毒通知]最新勒索病毒RANSOM_WANA.A攻擊以及趨勢科技防護策略
從: 趨勢科技 <info@edmb2b.trendmicro.com>
日期: 2017/5/13 上午 11:40
到: alan@mail.cyhg.gov.tw

2017年5月13日

最新勒索病毒RANSOM_WANA.A攻擊以及趨勢科技防護策略

趨勢科技發現最新的勒索病毒 WCRY（WannaCry）在全球各地的爆發案件，並已密切監控中。
初步分析顯示此勒索病毒是攻擊微軟的安全性弱點：MS17-010 – Eternalblue。而此安全性弱點與早先 Shadow Brokers 發布的駭客工具有關。
請參考下列趨勢科技部落格文章及病毒百科以獲取 WCRY 勒索病毒的變種及元件等相關資訊：

- 部落格：

  http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/

- 病毒百科：
  https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom_Wana.A

趨勢科技產品與防護措施

首先最重要的是此波攻擊是針對已知的微軟安全性弱點，請客戶透過 GPO 或是微軟官方的說明停用 SMB。此外，我們強烈建議您為作業系統安裝最新的修補程式，尤其是跟安全性弱點 MS17-010 相關的安全性修補程式。
趨勢科技建議您根據端點電腦、信件、伺服器、閘道、網路安全等等採用分層式防護以確保有效防禦各個潛在入侵點。在此基準上，我們已能針對這樣的新威脅事件提供某種程度的防護能力：

- 設定更新與下一代技術：
  趨勢科技客戶使用最新版本 OfficeScan 與 WorryFree Business Security 請確保已啟用「預測性機器學習」功能（OfficeScan XG 版本、Worry-Free Services、CloudEgde）以及所有與勒索病毒相關的防護功能。相關設定資訊請參考此則 KB 文章https://success.trendmicro.com/solution/1112223

- 病毒碼：
  趨勢科技已可偵測已知的病毒變種及元件，請確認您已更新病毒碼至下列版本：
  - 雲端病毒碼- 13.399.00
  - 傳統掃瞄病毒碼- 13.401.00

- 趨勢科技網頁信譽評等服務（Web Reputation Services，WRS）已加入已知的命令控制伺服器（Command and Control servers，C&C）。

- 趨勢科技 Cloud Edge 客戶請確認更新並套用以下規則
  - IPS Rules 1133635, 1133636, 1133637, 1133638 SMB Microsoft MS17-010 SMB Remote Code Execution。

- 趨勢科技 Deep Security 與 Vulnerability Protection已釋出了防堵此漏洞的規則更新。建議客戶儘快下載並套用至最新的規則更新
  - IPS Rules 1008224, 1008228, 1008225, 1008227 Includes coverage for MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities

- 趨勢科技 Deep Discovery Inspector客戶請確認已更新以下規則並監控是否偵測C&C連線
  - DDI Rule 2383:CVE-2017-0144 Remote Code Execution SMB (Request)

- 趨勢科技 TippingPoint客戶請確認已更新以下規則
  - Filters 5614, 27433, 27711, 27935, 27928 Includes coverage for MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities and attacks
  - ThreatDV Filter 30623 - helps to mitigate outbound C2 communication
  - Policy Filter 11403 - provides additional protection against suspicious SMB fragmentation

趨勢科技強烈建議，請務必儘速套用軟體廠商釋出的重大修補更新。若客戶和合作夥伴們需要進一步的資訊或是有任何方面的疑問，請您與趨勢科技技術支援部門聯繫取得進一步的協助。

[趨勢科技技術支援聯絡方式]

- 企業授權用戶技術專線: Tel: 886-2-2377-2323
- Web mail : http://www.trend.com.tw/corpmail/
- 產品技術問題請至常見問題集查詢
- 服務時間: 週一至週五 , 上午9:00~12:00 下午1:30 ~5:30 (例假日及國定假日除外)

—附件:

[新病毒通知]最新勒索病毒RANSOM_WANA.A.eml 23.8 KB